IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF (a) THE PERSON OF DEKLYN BUTLER (b) ROOM A232, BUILDING 11107, FORT GREGG-ADAMS, VA 23801	Case No. 3:23sw82 and 3:23sw83

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Matthew Marasco, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search of the person of DEKLYN BLAINE BUTLER (hereinafter referred to as "BUTLER"), as further described in Attachment A-1;and the premises located at Room A232, Building 11107, Fort Gregg-Adams, Virginia 23801 (hereinafter referred to as "PREMISES") as further described in Attachment A-2. In particular, this affidavit is made in support of an application for a warrant to search for and seize evidence, instrumentalities, and fruits of violations of 18 U.S.C. § 2252A(a)(5) Possession of Child Pornography, as further described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), United States Department of Justice, and have been since September 2019. I am assigned to the Richmond Field Office of the FBI in Richmond, Virginia, and am responsible for conducting investigations pertaining to child exploitation. As part of my duties, I have received training regarding the investigation of federal crimes including crimes against children, human trafficking, civil rights, and public corruption. By virtue of my employment with the FBI, I have

performed a variety of investigative tasks including, but not limited to, conducting arrests and executing federal search warrants. As a Special Agent, I am an investigative or law enforcement officer within the meaning of 18 U.S.C. § 2510(7).

3. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

RELEVANT STATUTORY PROVISIONS

4. **Possession of Child Pornography**: 18 U.S.C. § 2252A(a)(5) provides that it is a crime to knowingly possess, or knowingly access with intent to view, any child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

5. **Child pornography or Child abusive material** means any visual depiction, in any format, of sexually explicit conduct where: (A) the production involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital or computer-generated image that is substantially indistinguishable from that of a minor engaged in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

6. **Visual depictions** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which are capable of conversion into a visual image, and data which are capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

7. **Minor** means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

8. **Sexually explicit conduct** means actual or simulated: (i) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

TECHNICAL TERMS

9. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **Computer**, as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

b. **Storage Medium**: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

c. **Wireless Telephone**: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

d. **Smartphone:** A portable personal computer with a mobile operating system having features useful for mobile or handheld use. Smartphones, which are typically pocket-sized (as opposed to tablets, which are larger in measurement),

have become commonplace in modern society in developed nations. While the functionality of smartphones may vary somewhat from model to model, they typically possess most if not all of the following features and capabilities: 1) place and receive voice and video calls; 2) create, send and receive text messages; 3) voice-activated digital assistants (such as Siri, Google Assistant, Alexa, Cortana, or Bixby) designed to enhance the user experience; 4) event calendars; 5) contact lists; 6) media players; 7) video games; 8) GPS navigation; 9) digital camera and digital video camera; and 10) third-part software components commonly referred to as "apps." Smartphones can access the Internet through cellular as well as Wi-Fi ("wireless fidelity") networks. They typically have a color display with a graphical user interface that covers most of the front surface of the phone and which usually functions as a touchscreen and sometimes additionally as a touch-enabled keyboard.

e. **SIM Card**: Stands for a "subscriber identity module" or "subscriber identification module," which is the name for an integrated circuit used in mobile phones that is designed to securely store the phone's international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards.

f. **Log Files**: Records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

g. **Internet**: A global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

h. **Internet Protocol Address (IP address)**: A unique number used by a computer to access the Internet. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static–that is, long-term–IP addresses, while other computers have dynamic that is, frequently changed–IP addresses. Internet providers use either IP version 4 or more recently IP version 6. IPv4 is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Given the rapid growth of the volume of internet-enabled devices over the past two decades, in early 2011, the Internet Assigned Numbers Authority exhausted the global IPv4 free pool. As such, many providers switched to IPv6, which is a series of eight hexadecimal

digits, each separated by colons (e.g., FFE:FFFF:7654:FEDA:1245:BA98:3210:4562).

i. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage devices).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

10. As described above and in Attachment B, this application seeks permission to search for records that might be found on BUTLER's person and on the PREMISES, in whatever form they are found. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

11. **Probable Cause:** I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the storage medium that is not currently being used by an active file - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media - in particular, computers' internal hard drives - contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

12. **Forensic Evidence:** As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable

cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and

malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the

computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of

counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

13. **Necessity of Seizing or Copying Entire Computers or Storage Media:** In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and

configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

14. **Nature of Examination**: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of electronic devices, including cellular telephones, consistent with the warrant. The examination may require techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection to determine whether it is evidence described by the warrant.

15. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

PROBABLE CAUSE

I. INITIAL REPORT

16. In June 2021, the Criminal Investigation Division - Fort Lee Resident Agency (CID) located in Fort Lee, Virginia received information from the Cabot Police Department (CPD) in Cabot, Arkansas that Private DEKLYN BLAINE BUTLER, date of birth (DOB) January XX, 2003, then stationed at Fort Lee, Virginia (FLVA) (now Fort Gregg-Adams, VA), had exchanged sexually explicit images and videos with a 14-year-old minor female who resided in Cabot. The minor female disclosed the communication to her grandparents, who made the initial report to CPD.

17. On or about June 17, 2021, the minor female was forensically interviewed. During the interview, she disclosed that BUTLER added her randomly on the application Snapchat in December of 2020, and that the two began talking as friends. BUTLER stated he was 17 years old at the time, and she told him she was 14. Later in the conversation, BUTLER requested images of her breasts, to which she complied. The conversation between BUTLER and the minor female continued and included the exchange of various forms of sexually explicit messages, video chats, images, and videos. BUTLER threatened to ruin her life by sending out the images and videos of her if she did not send him more. The minor female complied with his requests and sent the additional images and videos. She stated BUTLER told her that he used some type of military program to find her and her grandparents, with whom she lives. Shortly thereafter, BUTLER texted the minor female's grandmother. The minor female confessed everything to her grandparents, who called CPD to report the incident.

II. INTERVIEW OF BUTLER AND FURTHER INVESTIGATION

18. On June 24, 2021, CID conducted a search of BUTLER's barracks room located at Fort Lee (now Fort Gregg-Adams) pursuant to a search warrant. During the search, CID seized several digital evidence items including BUTLER's cellular telephone, a Samsung Galaxy Note.

19. Additionally on June 24, 2021, BUTLER was interviewed by CID. During the interview, BUTLER admitted to exchanging sexually explicit messages, images, and videos with multiple minor females, including a 17-year-old minor victim residing in Minnesota, whom he communicated with on social media (hereinafter, MV1). BUTLER stated MV1 told him that she was 17 years old during the conversation. He described MV1 as a white female, approximately 140 pounds, residing in Minnesota. BUTLER stated he communicated with MV1 on Snapchat and Facebook, and that he saved the images and videos of MV1 in the gallery application on his cellular telephone as well as on Facebook. BUTLER also admitted to engaging in video calls with MV1, during which he asked MV1 to send images of her exposed buttocks, breasts, and vagina. BUTLER stated he shared depictions of his exposed penis and of himself masturbating several times with MV1. BUTLER stated the last time he spoke to MV1 was June 24, 2021.

20. Based on the information from the above interviews, CID conducted additional investigative steps including, but not limited to, serving legal process to Google, Facebook, Inc., Lightspace, Inc., and Snap, Inc for information associated with BUTLER's accounts, conducting interviews of identified potential victims and witnesses, and examining, and reviewing electronic devices belonging to BUTLER, as well as those belonging to several potential victims.

21. On September 28, 2021, CID obtained a search warrant for Snapchat account "deklynbutler19", which was previously identified as belonging to BUTLER.

22. During the course of the investigation, CID corroborated that BUTLER was engaged in sexually explicit online conversations with multiple female individuals, some of which were confirmed to be minors at the time.

23. In July 2022, CID contacted the FBI Richmond Field Office for assistance due to the complex nature and scope of the investigation. CID provided copies of all case documentation to the FBI.

24. Based on the information provided by CID, Butler is currently assigned to reside at the PREMISES, which is a barracks room located at Fort Lee (now Fort Gregg-Adams). The PREMISES is a dormitory-style room shared with approximately two to three other individuals, each having a designated bed, nightstand, and desk.

25. Because several people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

III. INTERVIEW OF MV1

26. On January 10, 2023, MV1 was interviewed at a local police department in Minnesota. During the interview, MV1 stated she met BUTLER on social media in the summer of 2021, when she was 17 years old, and communicated with him primarily on Snapchat and Facebook. When she first met BUTLER, he identified himself with his actual name, and even provided her with a picture of his driver's license. BUTLER told MV1 he was 18 years old, originally from South Carolina, and was employed with the United States Army in Virginia. MV1 advised that the first nude image or video she sent of herself to BUTLER was consensual, but that he requested it. MV1 felt comfortable with BUTLER, and he began asking for additional images and videos.

27. At some point, BUTLER told MV1 he would contact her parents if she did not send additional nude material of herself. MV1 complied with his requests and sent the additional images and videos, mostly through Snapchat.

28. At the conclusion of the interview, MV1 was shown 11 images previously obtained from BUTLER's electronic devices and social media accounts. The images were screenshots from larger video files depicting a female engaged in various sexual acts, namely masturbation. MV1 reviewed each image and confirmed that all were videos she took of herself in her bedroom at her residence in Minnesota. MV1 stated all of the videos were likely made during the same month based on the color of her hair dye and that she was a minor during that time.

IV. REVIEW OF SNAPCHAT COMMUNICATIONS

29. Law enforcement review of the Snapchat communications between BUTLER and MV1 revealed the exchange of multiple images and videos which were sexual in nature. For example:

a. On May 11, 2021, MV1 sent BUTLER "583aec24-8179-47-bc-ba38-5c92ace41784.mp4", an approximately 59-second video which depicts MV1masturbating with a black dildo.

b. On May 23, 2021, MV1 sent BUTLER "1bcb8258-e714-49f5-9204-fcbea25e6afa.mp4", an approximately 59-second video which depicts MV1masturbating with a black and white dildo, then placing the dildo in her mouth while continuing to masturbate with her fingers.

30. During this time, MV1 was 17 years old and BUTLER was stationed at and residing at Fort Lee, Virginia (now Fort Gregg-Adams, Virginia). Fort Lee, Virginia is within the special territorial jurisdiction of the United States.

V. REVIEW OF BUTLER'S CELLULAR TELEPHONE

31. Law enforcement review of BUTLER's cellular telephone, a Samsung Galaxy Note 20, Model SM-981U, which was seized from BUTLER by CID on June 24, 2021, pursuant to a search warrant, revealed several video files that appeared to be screen recordings from Snapchat conversations between BUTLER and MV1, who was 17 years old at the time. The screen recordings were sexual in nature. For example:

a. "Screen_Recording_20210605-221343_Snapchat.mp4", a video file of approximately three minutes and two seconds in length, depicts MV1 masturbating with her fingers. In a smaller window at the bottom of the screen, an unidentified male is observed masturbating simultaneously. Only the male's penis is visible.

b. "Screen_Recording_20210530-235052_Snapchat.mp4", a video file of approximately one minute and one second in length, depicts MV1 masturbating with a black dildo.

At the time the cellular telephone was seized, BUTLER was stationed at and residing at Fort Lee, Virginia (now Fort Gregg-Adams, Virginia).

BIOMETRIC ACCESS TO DEVICES

31. This warrant permits law enforcement agents to obtain from the person of DEVON BUTLER the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any devices requiring such biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

32. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device

through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

33. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

34. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

35. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward

the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

36. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

37. As discussed in this Affidavit, your Affiant has reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

38. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID or Face ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the

last 156 hours. Biometric features from other brands carry similar restrictions. With Apple devices, a passcode will be required if the phone has five failed attempts to unlock via Face ID. This is often reached by simply handling the phone during arrest or evidence inventory. In addition to device restart as mentioned above, the passcode will also be required after remote activation lock, or when the side or power buttons are pressed for longer than two seconds placing the phone in Emergency SOS mode. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

39. Due to the foregoing, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the aforementioned person the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the device(s) found at the PREMISES or on BUTLER's person; (2) hold the device(s) found at the PREMISES or on BUTLER's person in front of the face of the aforementioned person(s) to activate the facial recognition feature; and/or (3) hold the device(s) found at the PREMISES or on BUTLER's person in front of the face of the aforementioned person(s) to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant. The proposed warrant does not authorize (nor does it prohibit) law enforcement to request that the aforementioned person state or otherwise provide the password or any other means that may be used to unlock or access the device(s). Moreover, the proposed warrant does not authorize (nor does it prohibit) law enforcement to ask

the aforementioned person to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the device(s). That is, if agents in executing the warrant ask the aforementioned person for the password to any device(s), or to identify which biometric characteristic unlocks any device(s), the agents will not state or otherwise imply that the warrant requires such person to provide such information; that is, the agents will make clear that any such request is voluntary/the person is free to refuse the request.

CONCLUSION

32. Based on the forgoing, I submit there is probable cause to believe that BUTLER's person, as further described in Attachment A-1; and the PREMISES, as further described in Attachment A-2, contain evidence and instrumentalities of violations of 18 U.S.C. § 2252A(a)(5) Possession of Child Pornography, as further described in Attachment B.

Respectfully submitted,

Matthew Marasco
Special Agent
FBI Richmond Field Office

SUBSCRIBED and SWORN before me this 2nd day of June 2023.

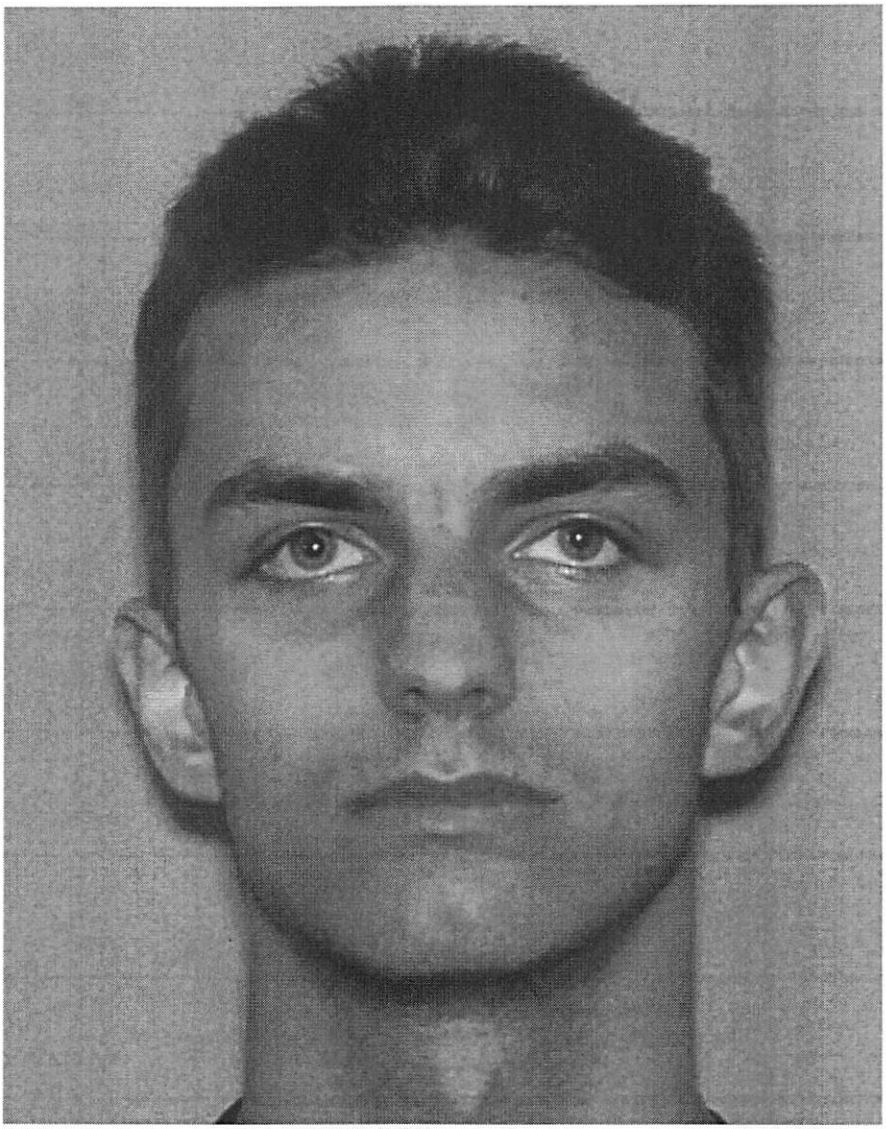
/s/ MRC
Mark R. Colombell
United States Magistrate Judge

Honorable Mark R. Colombell
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A-1

Property to Be Searched

The person to be searched is DEKLYN BUTLER, a male born on January XX, 2003, with blonde hair and approximately 6'0" tall, including all personal items and containers, including electronic devices, in his physical possession, on his person, or in areas within his immediate control.



ATTACHMENT A-2

Property to Be Searched

The property to be searched is Room A232, Building 11107, Fort Gregg-Adams, Virginia 23801 (the "PREMISES"). The PREMISES is a dormitory room located inside a troop barracks and company area of operations building with five floors. There are no more than three soldiers residing in each room, which typically contains three desks, three beds, three nightstands, three lockers/closets, and a shared bathroom area. This warrant applies to the areas belonging to BUTLER, as well as common areas to which BUTLER has access.

ATTACHMENT B

Particular Things to be Seized

1. All records relating to violations of 18 U.S.C. § 2252A(a)(5) Possession of Child Pornography, including:

   a. Any and all visual depictions of minors;

   b. Any and all address books, names and lists of names and addresses of minors;

   c. Any and all records reflecting physical contacts, whether real or imagined, with minors; and

   d. Any and all child erotica, including photographs of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids.

2. Computers, electronic devices, or storage media used as a means to commit the violations described above.

3. For any computer, electronic devices, or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondences;

   b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. Evidence of the lack of such malicious software;

   d. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

   e. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER.

   f. Evidence of the times the COMPUTER was used;

   g. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. Records of or information about Internet Protocol addresses used by the COMPUTER;

j. Records of, or information about, the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

k. Contextual information necessary to understand the evidence described in this attachment.

During the execution of the search of BUTLER's person and the PREMISES, as further described in Attachments A-1 and A-2, law enforcement personnel are also specifically authorized to obtain from BUTLER the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person's physical biometric characteristics will unlock the device(s), to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition of:

(a) any of the device(s) found at the PREMISES or on BUTLER's person,
(b) where the device(s) are limited to those which are capable of containing and reasonably could contain fruits, evidence, information, contraband, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant Attachments A-1 and A-2,

for the purpose of attempting to unlock the device(s)'s security features in order to search the contents as authorized by this warrant.

While attempting to unlock the device by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person state or otherwise provide the password or identify the specific biometric

characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the device(s). Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person is permitted. To avoid confusion on that point, if agents in executing the warrant ask the aforementioned person for the password to any device(s), or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any device(s), the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no previous or future involvement in the investigation of this matter. The Filter Team will review all seized communications and segregate potentially protected

materials, i.e. communications to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team decides that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.

Your affiant requests the search warrant for the aforementioned items to include the opening and searching of any locked safes, boxes, and compartments.